Community Scheme Protection of Personal Information Policy

Introduction This document outlines the policies for protecting personal information in compliance with the Protection of Personal Information Act, 4 of 2013 (POPIA) and the Promotion of Access to Information Act, 2 of 2000 (PAIA). These policies aim to safeguard individuals' privacy rights within the scheme.

Key Definitions

- **Consent**: Voluntary, specific, and informed agreement to process personal information.
- **Information Officer**: Appointed person responsible for ensuring compliance with POPIA and PAIA.
- **Personal Information**: Any information linked to an individual or juristic person.
- **Processing**: Collecting, using, storing, sharing, retaining, and/or destroying personal information.
- **Community Scheme**: Relates to the complex for which this policy applies.
- **Scheme Executives**: This refers and includes trustees/directors/committee members/board members.
- **Solver**: Any reference to Solver relates to our preferred managing agent which is Solver Property Services.

Applicability These policies apply to all personal information processed by the scheme and any requests for access to such information. They do not override POPIA or PAIA, and in case of conflict, the latter will prevail.

Disclaimer This document has been prepared with the assistance of Solver Property Services. Scheme Executives acknowledge that, while this manual is provided free of charge for existing clients as a general and compressed policy, Solver Property Services accepts no liability for its use. The decision to utilise this manual is at the sole discretion of the user. For a more detailed and comprehensive policy, Community Schemes are encouraged to consult with legal professionals.

Information Officer and Deputy Information Officer

- **Appointment**: Scheme Executives will appoint an Information Officer and may appoint Deputy Information Officers. If not formally appointed, this will default to the Chairperson being the Information Officer and the Treasurer/Finance Scheme Executive being the Deputy Information Officer.
- **Responsibilities**: Ensuring compliance with POPIA and PAIA, conducting gap analyses, and implementing necessary changes.

Processing and collecting of Personal Information

We may collect or obtain personal information about you:

- Directly from you.
- In the course of our relationship with you.
- When you make your personal information public.
- When you visit and/or interact with our website or social media platforms.
- When you register to use any of our services.
- When you interact with third-party content or advertising on our website.
- When you visit our offices.
- From third parties (e.g., law enforcement authorities).
- Through records of your communications and interactions with us.

Categories of Personal Information We May Process

In terms of POPIA, the scheme may process the following categories of personal information about you:

- **Personal Details:** Name and photograph.
- **Demographic Information:** Gender, date of birth/age, nationality, salutation, title, and language preferences.
- **Identifier Information:** Passport or national identity number, utility provider details, bank statements, tenancy agreements.
- **Contact Details:** Correspondence address, telephone number, email address, and details of your public social media profiles.
- **Instruction Details:** Personal information included in correspondence, documents, evidence, or other materials that we process in the course of providing services to you.
- **Attendance Records:** Details of meetings and other events organized by or on behalf of the scheme that you have attended.
- **Consent Records:** Records of any consents you may have given, together with the date and time, means of consent, and any related information.
- **Payment Details:** Billing address, payment method, bank account number or credit card number, invoice records, payment records, SWIFT details, IBAN details, payment amount, payment date, and records of cheques.
- **Data relating to your visits to our website:** Device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a website, and other technical communications information.
- **Employer Details:** Where you interact with us in your capacity as an employee of an organization, the name, address, telephone number, and email address of your employer, to the extent relevant.
- **Content and Advertising Data:** Records of your interactions with our online advertising and content, records of advertising and content displayed on pages displayed to you, and any interaction you may have had with such content or advertising.

Sensitive Personal Information Where we need to process your sensitive personal information, we will do so in the ordinary course of our business, for a legitimate purpose, and in accordance with applicable law.

Conditions for Lawful Processing

1. **Accountability**: The scheme will process personal information lawfully and transparently.
2. **Processing Limitation**: Information will be processed only for specific, lawful purposes.
3. **Purpose Specification**: Information will be collected for defined purposes and not retained longer than necessary.
4. **Further Processing Limitation**: Secondary processing will be compatible with the original purpose.
5. **Information Quality**: Information will be accurate, complete, and updated as necessary.
6. **Openness**: The scheme will maintain transparency about its information processing practices.
7. **Security Safeguards**: Technical and organisational measures will be implemented to protect information.

Rights of Data Subjects

- **Right to be Informed**: Individuals have the right to know the purpose of processing their information.
- **Right to Withdraw Consent**: Consent can be withdrawn at any time, and the scheme will remove the information.
- **Right to Correct Information**: Individuals can request corrections to their personal information.
- **Right to be Notified of Breaches**: Individuals will be informed of any security breaches affecting their information.

Scheme Executives and Information Officer's Rights

(This extends to Solver Property Services who acts on behalf of the community scheme)

- **Processing Without Consent**: Certain personal information can be processed without consent for legal or contractual reasons.
- **Refusal of Information Transmission**: Requests for personal information will be assessed to balance privacy rights and the scheme's management needs.
- **Refusal of Admission**: Visitors may be denied entry if they refuse to provide necessary personal information.

Purposes of Processing and Legal Bases for Processing

The scheme will process your personal information in the ordinary course of the business of the scheme. We will primarily use your personal information only for the purpose for which it was originally or primarily collected. We may use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which the personal information was collected. We may subject your personal information to processing during the course of various activities, including, without limitation, the following:

- Operating our business.
- Compliance with the Sectional Titles Schemes Management Act or the Companies Act
- Compliance with any other applicable law and fraud prevention.
- Transfer of information to our service providers and other third parties.
- Relationship management and marketing purposes in relation to our services.
- Internal management and management reporting purposes.
- Safety and security purposes.
- Day-to-day operations.

Dispute Resolution and Information Regulator

- **Complaints**: Individuals can submit complaints about personal information breaches.
- **Escalation**: Complaints can be escalated to the Information Regulator if internal remedies are exhausted.

Amendments and Compliance

- **Amendments**: Policies will be updated automatically with changes in legislation or by Scheme Executives' resolution.
- **Compliance**: The scheme will ensure compliance with POPIA and PAIA through regular reviews and updates.

Operational Considerations

- **Monitoring**: The Information Officer is responsible for administering and overseeing the implementation of this policy and supporting guidelines, standard operating procedures, notices, consents, and appropriate related documents and processes.
- **Training**: All employees, residents, representatives, service providers, and individuals directly associated with the scheme are to be trained in the regulatory requirements, policies, and guidelines that govern the protection of personal information.
- **Reviews and Audits**: Periodic reviews and audits will be conducted to ensure compliance with this policy and guidelines.

Disclosure of Personal Information to Third Parties

We may disclose your personal information to our associates and service providers for legitimate business purposes, in accordance with applicable law and subject to applicable professional and regulatory requirements regarding confidentiality. In addition, we may disclose your personal information:

- If required by law.

- To regulatory authorities, upon request, or for the purposes of reporting any actual or suspected breach of applicable law or regulation.
- To third-party operators (including data processors such as providers of data hosting services and document review technology and services), located anywhere in the world, subject to certain conditions.
- Where it is necessary for the purposes of, or in connection with, actual or threatened legal proceedings or establishment, exercise, or defence of legal rights.
- To any relevant party for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- To any relevant third-party provider, where our website uses third-party advertising, plugins, or content.

Operating Controls

- **Information Security Responsibilities**: Allocation of information security responsibilities.
- **Incident Reporting and Management**: Procedures for reporting and managing incidents.
- **Information Security Training and Education**: Regular training and education on information security.
- **Policy Compliance**: Any breaches of this policy may result in disciplinary action and possible termination of employment or legal action.

Data Accuracy and Minimisation

The personal information provided to the scheme should be accurate, complete, and up-to-date. Should personal information change, the onus is on the provider of such data to notify the scheme of the change and provide the scheme with the accurate data. The scheme will restrict its processing of personal information to data which is sufficient for the fulfilment of the primary purpose and applicable legitimate purpose for which it was collected.

Direct Marketing

We, Solver Property Services, and/or any of our employees/service providers the may process your personal information for the purposes of providing you with information regarding services that may be of interest to you. You may unsubscribe for free at any time. If you currently receive marketing information from us which you would prefer not to receive in the future, please email us at the provided contact details.

Conclusion

These policies are enacted to protect personal information and ensure compliance with relevant legislation. The scheme is committed to maintaining the privacy and security of all personal information it processes.

Gap Analysis						
	Which Information is collected:	**Who collects and/or has access to such information**	**Purpose of collecting such information**	**Existing safeguards for such information?**	**Forceble Breaches**	**Prevention Meathods**
1	Full Names	Solver Property Services as the managing agent; The Executive Committee Members, and at times the auditors, tax practitioners, compliance support staff, on site managers and the owners in the complex	Compliance with legislation (Ie. STSMA, Companies act etc)	Solver Property Services has antivirus software and firewalls. The staff are also trained. Data is handled sensitively. Implement role-based access to sensitive information. Requirements for employees clear their desks of sensitive information at the end of the day. Collect only the necessary personal information. Regularly review and delete unnecessary data.	Attackers use automated tools to guess passwords by trying numerous combinations until the correct one is found. This can be particularly effective against weak or commonly used passwords1.	Enforce the use of complex passwords that include a mix of letters, numbers, and special characters.
2	Identity / Passport Number				Potential phishing attacks	Solver conduct basic training sessions to help employees identify risks.
3	Section Address				Employees or former employees with access to sensitive information misuse their access to steal or leak data	Solver to implement access controls.
4	Telephone Number				Attendance register at Annual General Meeting	Solver staff to try and keep the attendance register with the owners personal information with them at all times.
5	Email Address					
6	Mailing Address					